Chapter 15
Futuristic Image Processing Techniques to Ameliorate Data Security and Privacy in Kidney Health Studies

Lakshya Pandey
http://orcid.org/0009-0005-2468-4237
VIT Bhopal University, India

Spandan Agrawal
http://orcid.org/0009-0008-0013-2739
VIT Bhopal University, India

D. Lakshmi
http://orcid.org/0000-0003-4018-1208
VIT Bhopal University, India

Ananya Chandorkar
Walt Disney Company, USA

ABSTRACT

Deep Learning (DL) is well-suited for handling big data challenges and future issues in IoT. Advanced image processing techniques are pivotal in addressing security challenges in medical imaging. Anonymization techniques, encryption, watermarking, and Federated Learning (FL) are crucial for securing data and protecting privacy. AI-driven Clinical Decision Support Systems (CDSS) are increasingly used

DOI: 10.4018/979-8-3373-7426-0.ch015

in clinical medicine, integrating Machine Learning (ML) capabilities into expert systems to enhance performance. The Unlearning Technique has recently become a way to implement the concept of "the right to be forgotten" in FL. Current research on effective retraining or approximate unlearning methods often overlooks the information leakage risks tied to model differences before and after unlearning.

1.0 INTRODUCTION

The growing reliance on digital imaging technologies—such as X-rays, Magnetic Resonance Imaging (MRI), and digital pathology slides—has significantly transformed the medical field. However, this advancement has also introduced critical challenges related to data privacy, image integrity, and cybersecurity. Sensitive medical images often contain identifiable patient information, making them vulnerable to cyberattacks and unauthorized access. In disciplines like nephrology, where diagnostic and monitoring processes heavily depend on imaging modalities such as ultrasound, CT scans, and MRIs, ensuring the security and confidentiality of patient image data has become a major concern (Toch et al., 2018). To tackle these challenges, FL and Machine Unlearning (MU) have emerged as essential solutions. FL enables collaborative model training across multiple healthcare institutions without the need to share raw patient data, thereby preserving privacy while enhancing diagnostic accuracy. This decentralized approach ensures that sensitive medical images remain securely stored within their local environments, thereby minimizing the risk of data leakage. Meanwhile, MU enhances data governance and compliance by allowing for the selective removal of certain data contributions from trained models—an important capability for maintaining regulatory compliance and protecting patient rights under frameworks like GDPR and HIPAA. Integrating these privacy-preserving technologies aligns with the broader evolution of AI-driven healthcare analytics. Here, big data and advanced ML techniques are transforming CDSSs (CDSS). AI-powered CDSS combine expert systems with data-driven models to assist clinicians in diagnosis and treatment planning, leveraging large datasets while ensuring patient data security (Yang et al., 2019). The inclusion of FL and unlearning mechanisms strengthens these systems by enhancing trust, transparency, and resilience against data breaches. As healthcare systems increasingly adopt digital and AI-based tools, it becomes crucial to implement robust frameworks that not only enhance analytical accuracy but also uphold ethical standards of data privacy, fairness, and accountability. Advanced privacy-preserving techniques like FL and unlearning represent a significant step toward securing sensitive medical image data while enabling innovation in intelligent healthcare applications (Nwobodo et al., 2024; Al-Ghaili et al., 2023). In short, combining FL's privacy-preserving col-